AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for conveying a security context, comprising:

creating and assigning a virtual address to a client process;

issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context, and wherein data in the first Internet Protocol version compliant packet is encrypted using the security context;

prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet, wherein the first Internet Protocol version is different than the second Internet Protocol version;

forwarding the second Internet Protocol version compliant packet to a recipient;

stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;

decrypting and authenticating data within the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and

routing the decrypted and authenticated packet to a recipient process using the virtual address.

2. (Original) The method of claim 1, wherein the first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet.

3. (Original) The method of claim 1, wherein the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet.

4. (Original) The method of claim 1, wherein issuing the packet further comprises:
   executing a Supernet Attach Command with an authentication server daemon;
   responding to the Supernet Attach Command with a Supernet configuration information comprising the security context in the address; and
   registering a mapping of the Supernet configuration information with a virtual address daemon.

5. (Original) The method of claim 1, wherein the security context in the address comprises the virtual address, a Supernet identity, and a channel identity.

6. (Original) The method of claim 5, wherein the security context comprises a 128 bit unique value.

7. (Original) The method of claim 6, wherein the security context comprises a 16 bit set and a 112 bit set.

8. (Original) The method of claim 7, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.

9. (Original) The method of claim 7, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.

10. (Original) The method of claim 7, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.

11. (Original) The method of claim 4, wherein the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address.

12. (Original) The method of claim 1, wherein the security context is encoded.

13. (Original) The method of claim 1, wherein the security context is obtained from the stripped packet using a handler mechanism.

14. (Cancelled)

15. (Currently Amended) A network system comprising:

an authentication server daemon that replies to a Supernet Attach Command; and

a virtual address daemon that maintains a mapping of the Supernet configuration information performing the following steps:

creating and assigning a virtual address to a client process;

issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context, and wherein data in the first Internet Protocol version compliant packet is encrypted using the security context;

prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet, wherein the first Internet Protocol version is different than the second Internet Protocol version;

forwarding the second Internet Protocol version compliant packet to a recipient;

stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;

decrypting and authenticating data within the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and

routing the decrypted and authenticated packet to a recipient process using the virtual address.

16. (Original) The method of claim 15, wherein the first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet.

17. (Original) The method of claim 15, wherein the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet.

18. (Original) The network system of claim 15, wherein issuing the packet further comprises:
executing a Supernet Attach Command with an authentication server daemon;
responding to the Supernet Attach Command with a Supernet configuration information comprising the security context in the address; and
registering a mapping of the Supernet configuration information with a virtual address daemon.

19. (Original) The network system of claim 18, wherein the security context in the address comprises the virtual address, a Supernet identity, and a Channel identity.

20. (Original) The network system of claim 19, wherein the security context comprises a 128 bit unique value.

21. (Original) The method of claim 20, wherein the security context comprises a 16 bit set and a 112 bit set.

22. (Original) The method of claim 21, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.

23. (Original) The method of claim 21, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.

24. (Original) The method of claim 21, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.

25. (Original) The method of claim 18, wherein the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address.

26. (Original) The method of claim 15, wherein the security context is encoded.

27. (Original) The method of claim 15, wherein the security context is obtained from the stripped packet using a handler mechanism.

28. (Cancelled)

29. (Currently Amended) An apparatus for conveying a security context, comprising:

means for creating and assigning a virtual address to a client process;

means for issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context, and wherein data in the first Internet Protocol version compliant packet is encrypted using the security context;

means for prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet, wherein the first Internet Protocol version is different than the second Internet Protocol version;

means for forwarding the second Internet Protocol version compliant packet to a recipient;

means for stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;

means for decrypting and authenticating data within the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and

means for routing the decrypted and authenticated packet to a recipient process using the virtual address.